TECHNICAL REPORT

ISO/IEC TR 30125

First edition
2016-05-01

Information technology — Biometrics used with mobile devices

Technologies de l'information — Biométrie utilisée avec des appareils mobiles

Reference number
ISO/IEC TR 30125:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 37, *Biometrics*.

Introduction

The widespread use and capability of mobile technology has created a demand for people to be able to conduct their personal and business lives on the move in a way that previously would have been limited to the home and office environments. To service this demand, mobile communications, applications and transactions need to be protected to safeguard the privacy of the user and to ensure the integrity of the transaction. This is essential for creating a trusted mobile platform environment in which individuals, businesses, non-profit organizations and governments can transact. User authentication, being sure that you are dealing with the right person, is a vital part of this and one that poses particular difficulty when the user is communicating from an unknown remote location. The potential for impersonation and fraud is high.

User authentication is commonly achieved through the use of a username and password. This approach uses only one category of credentials, the password, and is referred to as Single Factor Authentication (SFA). Use of a biometric instead of a password is another example of SFA. For mobile applications that require high levels of security, policy may require the use of more than one credential. Use of more than one credential is referred to as Multi Factor Authentication (MFA). Multi-factor authentication can be accomplished with one or more of the following:

a) something you know (e.g. password);

b) something you have (e.g. identity card);

c) something you are (e.g. face, fingerprints, iris).

Authentication, in providing assurance that a person is who they say they are, can be improved through the use of biometric recognition. Other forms of identification, such as tokens or passwords, are not closely bound to an individual in the same manner as a biometrics is, and provide greater opportunity for substitution or theft. Password and token authentication authenticates the password or the token not the person and the authentication assurance is limited by the level of trust that exists that the password or token is being presented by the legitimate user and has not been acquired by an impostor.

The range of mobile devices and communication channels involved in mobile transactions is large and variable. Smart phones, tablets, laptops and other smart devices based on embedded systems are common examples of mobile devices and the Internet and Global System for Mobile communications (GSM) are examples of communication channels. Mobile devices are often owned by their users but not always; they could be company owned and supplied to employees for their own use.

A number of mobile device manufacturers produce units containing sensors. Conceivably, these sensors could be used to collect biometrics [i.e. camera for face, touch screen for finger or palm, microphone for voice, Global Positioning System (GPS) and accelerometers for gait]. Applications built for mobile platforms may use these sensors to capture biometrics for purposes such as authentication.

This Technical Report addresses the use of biometrics in scenarios where a person is mobile and wants to connect to a specific service irrespective of the device type and communication channel.

There are three key issues to consider when biometrics are used in such scenarios.

— The biometric capture environment – application developers will require a means of taking into account the uncontrolled nature of the capture environment. The uncontrolled capture environment will most likely mean that it is not possible for capture conditions to conform to the 'best practice' constraints for biometric capture (e.g. pose, background, etc.) set out in current biometric standards; and also require recognition algorithms and/or thresholds to be modified to take account in the case of reduced quality of biometric capture if the application can be compliant with reduced security.

— Biometric data privacy and security implications – the distribution of biometric data to commercial devices with security weaknesses and storage of biometric data in third-party cloud implementations. In this Technical Report, these security and privacy issues are addressed by referencing other standards where available noting that work is ongoing in establishing benchmarks and 'best

practice' to safeguard information including personal information. Definition of standards for security in mobile devices is not in the scope of this Technical Report.

— Biometric authentication - relative consistency of approach to biometric authentication across all application developers to ensure 'best practice' and consistent 'look and feel' for users." (More information may be found in NISTIR 8003).

Current biometric standards and associated security standards for biometrics do not yet adequately address the issues raised with the use of biometric capture on commercial computing devices, with distribution of biometric data via 'the cloud'. Work is still required in establishing benchmarks and 'best practice'.

This Technical Report is aimed at all parties with an interest in offering biometric functions or a biometric framework for use on mobile platforms including developers of third-party open source software libraries. It is also intended to provide a reference document for standards developers seeking to develop standards for the use of biometrics in mobile environments.

Information technology — Biometrics used with mobile devices

1 Scope

This Technical Report provides guidance for developing a consistent and secure method of biometric (either alone or supported by non-biometric) personalization and authentication in a mobile environment for systems procured on the open market.

Guidance is provided for

— 1:1 verification or 1:few positive identification;

— biometric sample capture in the mobile environment where conditions are not well controlled and not covered in ISO/IEC Biometric interchange format standards and the ISO/IEC Biometric sample quality Technical Reports;

NOTE 1 Further information regarding architectures may be found in NIST/SP 500-288.

— the best use of multiple biometric and non-biometric (PINs, passwords, personal data) personalization and authentication methods (i.e. multifactor).

NOTE 2 More information may be found in ISO/IEC 30108-1.

This Technical Report defines a framework to address methods and approaches for remote and unsupervised enrolment, together with secure storage and transmission of biometric and supporting biographic data, covering a variety of both online connected and offline modes.

This Technical Report identifies the functional elements and components of a generic mobile biometric system and the distinct characteristics of each component. It provides guidance related to a generic mobile architecture with reference to supporting standards.

The context recognizes a) the user as being mobile and b) operation across a variety of platforms, particularly mobile devices but also including tablet, laptop and other personal computing devices. The key to defining this context is whether the user's environment is physically controlled by the organization to which the user seeks access.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37[1)], *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and the following apply.

1) For a freely available copy of ISO/IEC 2382-37:2012, see: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

3.1
mobile device
small, compact, handheld, lightweight computing device, typically having a display screen with digitizer input and/or a miniature keyboard

Note 1 to entry: Examples include laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets.

3.2
personalization
ability to configure for a device to react in particular way for a specific individual

4 Abbreviated terms

BI Biometric interface

GPS Global Positioning System

GUI Graphical user interface

LAC Logical access control

NFC Near field communication

OS Operating system

OTG On-the-go – the USB connector of a smartphone

SE Secure element

TEE Trusted execution environment

USB Universal Serial Bus

5 The use of biometrics in mobile devices

5.1 Taxonomy of usage of biometrics in mobile devices

5.1.1 General

The context in which mobile devices can be used may be categorized, at a high-level, into four generic Use Cases. In all cases, usability and human factors should be considered and integrated into the development process of an application with use of biometric capability.

5.1.2 Generic considerations for all use cases

It is important to take account of the level of assurance required by providers and users of services in a mobile environment. These will depend on the nature of the service and environmental factors such as location, degree of remote control (if any), time, cryptographic and other security protection processes. Because the analysis of the security and assurance level is out of the scope of this Technical Report, the following clauses simply refer to high, medium and low levels of assurance. More detailed information on this aspect can be found in ISO/IEC 29115.

When implementing biometric services in mobile devices, it is important to note that irrespective of the biometric which is used or the application which uses it, the following functions should be considered:

a) capture of a biometric sample;

b) storage of a biometric reference (in some cases, this may be remote from the mobile device);

c) processing of biometric samples;

d) comparison of a biometric sample with a biometric reference (which may be remote from the device).

These general functionalities require some basic functions including:

a) capturing one or more biometric sample(s) from a sequence of samples (i.e. a facial image from a live view of a face);

b) establishing the best sample(s) based on some quality metric;

c) providing feedback to donor/subject for presentation of biometric (e.g. oval shape to position face);

d) providing a quality metric for sample capture;

e) providing feedback for failure to capture/failure to enrol;

f) providing information on what sensors are available on device (e.g. camera, multi-touch screen, finger scanner, GPS, accelerometer, etc.) together with any relevant technical details (e.g. touch screen resolution, number of multi-touches, camera resolution, etc.);

g) providing information on what biometric modalities have been captured as references;

h) comparison algorithms for each modality 1:1 and/or 1:few;

i) pass comparison score or pass fail result.

The application itself could handle some further biometric functions and fundamental identity management functions, such as:

a) ability to capture a new identity, delete or update an identity;

b) ability to handle exceptions;

c) processing of biometric samples.

These functions could form part of the OS framework. Consideration needs to be given to what elements may be resident on the device and what data may be processed remotely [e.g. via a web service, REST (Representable State Transfer), HTTP GET (Hypertext Transfer Protocol Group Encrypted Transfer), XML-RPC (Extensible Markup Language - Remote Procedure Call), etc.]. Different approaches may be taken in different circumstances, even for the same application. The device may be connected or not connected. At the platform level the user should see consistency in their interface.

Biometric comparison may be performed in the device or passed off to a remote server, depending on the use case and level of trust required.

A key aspect of mobile applications is the uncontrolled nature of the environment. The environment is one which is not controlled by the service the person is trying to access, so level of trust will be an important factor. Also, the environment could be different for each access occasion and vary over time.

In addition, it may be beneficial to use remote processing at a variety of system component interfaces. This would not only improve interoperability but allow biometric capabilities into systems that might not otherwise have them available. For example, an acquisition service such as WS-Biometric Devices (Web Services-Biometric Devices) would allow a mobile device without a built-in fingerprint scanner to acquire fingerprints from such an enabled scanner. A standard web service such as BIAS (Biometric Identity Assurance Service) may do the same for enrolment or recognition; for example, in cases where the data or comparison capabilities are not available locally. [Further information may be found in NIST/SP 500-288].

In any of the cases, certain general considerations should be addressed.

a) A decision should be taken on how the enrolment is performed, either in a supervised manner (external validation of the sample/s provided by some means) or in an unsupervised way (the user self-assesses the enrolment, with or without some quality check features on standards).

   In the case of unsupervised enrolment, it is recommended that the enrolment system automatically checks the quality of the samples provided (e.g. by following the relevant part of ISO/IEC 29794) and, when several samples are provided, the completeness of the union of all samples.

b) In order to protect the personal data of the device user it is recommended that both, the generation, and storage of the biometric probes and references, are protected so that there is no external access to these (e.g. from a third party application).

c) Although typically the device is to be operated by a single user, the possibility of more than one person using the device should be analysed with respect to the impacts of this on the device and assurance levels.

d) The computational power of a mobile device is expected to be less than that of a desktop computer or server. Therefore, analysis of the mobile device's biometric processing performance, given the resources available to the device, is recommended. Analysis should also be conducted on the performance of any sensor or biometric capture component built into the mobile unit, where the features of a built in capture component are comparably less than the feature set of an equivalent, specialist, stand-alone capture device.

e) Biometric services may be provided by the OS or by a third party application. In either case, the biometric services should run within a 'sandbox' to limit the possibility of the biometric services running malicious code or accessing configuration data which affects the service's behaviour (e.g. decision thresholds).

5.1.3 Access to the device

This is a service offered locally at the device without the need of using on-line services. Typically, the decision is performed at the device itself, and a positive outcome will unlock the device and allow the user to access the rest of the services and applications installed in the device or offered remotely.

EXAMPLE Examples include using a personal biometric instead of a password, PIN or graphical pattern to unlock the device when it is turned on, or after a period of inactivity.

This service provides a minimum level of assurance to the device and the data and applications included. Applications and particular data access may require further authentications, which will raise the level of assurance. As the user of the device may want to access low assurance services (e.g. reading the news on a public newspaper), the mechanism of unlocking the devices should address convenience more than security, and, therefore, the level of assurance for this kind of use should be considered as low. The organization providing the device may consider raising such assurance level as to gain a more rigid control on the use of the device.

For user convenience in low security scenarios, after a fixed number of failed attempts, the device could offer an alternative modality or method (e.g. a password, PIN or graphical pattern could be offered as an alternative unlocking means).

5.1.4 Access to the local applications, services and/or data

This is a service offered locally at the device without the need of using on-line services. Typically, the decision is performed at the device itself, and requested by an application in order to allow continuing use of the application, or access to certain services, or control of the access to particular protected data. This should only be executed with the device unlocked and only by the application accessible at the main screen, to avoid unauthorized access by third-party applications or services.

EXAMPLE Examples include accessing a protected folder in the internal memory of the device, through a particular file explorer application.

The level of assurance required in this case depends on the application trying to authenticate the user, and the step to be accessed. Therefore, the level of assurance may change from one application to another. This means that thresholds (e.g. quality or comparison thresholds) may have different values depending on the assurance level demanded. In order to avoid misuse by third-party applications, consideration should be given to restricting the values of the thresholds so that they do not block the system nor pass everybody. The absolute miss threshold should never overlap the absolute hit threshold.

NOTE It is possible that the biometric service manufacturer may not be willing to provide different assurance levels, having fixed thresholds for its operation.

5.1.5 Access to the communications channel

This is an on-line mode of operation analogous to the situation of the previous case, but where the service or data to be accessed is located in a remote system. In this case the device is attempting to go on-line and open a communications channel to authenticate itself digitally to, and register on, that channel before being granted access. Instead, or in addition, biometric recognition may be used to authenticate the device user to the communications channel.

EXAMPLE Examples include verifying that a particular user is entitled to use a particular communications channel by the operator/owner of that channel, amongst other things for automatically implementing billing, credit and access policy.

Possible variations include:

a) local biometric authentication is used via some version of the mechanism described above, to release an authentication token that the communication channel trusts,

b) a biometric token is produced locally which is authenticated remotely by the system controlling access to the communications channel,

c) a biometric sample is sent to the remote system controlling access to the communications channel for processing and authenticated remotely against its enrolled user database,

d) federated systems where parts of data from more than one trusted source are combined.

When developing this kind of use case, the same considerations as in 5.1.3 should be taken into account, and, additionally, the following:

— identification mode or verification mode - processes may or may not be required to include an identity claim, e.g. device identifier such as IMEI (International Mobile Station Equipment Identity) number, or personal identifier via data stored on the device;

— validity duration of the authentication for the communications channel.

5.1.6 Verification/authentication of, or to, a remote resource or point of transaction

This is an on-line mode which may share the functional qualities of the processes described in 5.1.4, but where the owner/controller of the remote asset regards as insufficient or irrelevant the fact that the communications channel has already been authenticated.

EXAMPLE Examples may include situations where the communications channel has not been biometrically authenticated, and where the access policy and trust levels required are different from those of the communications channel provider. This might typically exist where a communications channel provides the carrier for a VPN (Virtual Private Network) service.

Consideration should be given to the security level achieved by the communication channel which may be reduced over time, therefore the biometric information exchanged, if any, should be additionally protected over the communication protocol.

5.2 Generic challenges in the integration of biometrics in mobile devices

5.2.1 Computational power

In the past, the lack of computational power of portable devices was one of the reasons for not considering viable the integration of several biometric modalities. But nowadays, after the spread of the new generation of 32-bit low power consumption microprocessors, this challenge is no longer such. In particular, if we consider that the computation needs will happen or be required when processing the biometric information inside the devices, it will only occur when using a one to one comparison (i.e. sample vs. biometric reference stored in the device), or as much, one to few comparisons, if there are several biometric references enrolled in the device. One to many comparisons can be run directly on a mobile device, but are more likely to be run on a central server, using a biometric sample acquired through the mobile device.

Sample acquisition and feature extraction may take considerably more time than comparison, especially in a 1:1 scenario. Also, for some modalities, implementations might code and compare features from every available frame so consideration should be given to processing extraction and comparison in real time.

There have been successful implementations of biometric modalities in mobile devices with examples being: fingerprint,[1] iris,[2] face,[3] hand,[4] voice,[5] and signature.[6] While processing does take longer due to limited processing power, in all cases, there has been no increase in reported error rates when compared to implementations on desktop computers. The provider should validate that the error rate has not changed.

5.2.2 Data protection and privacy

Currently, a mobile device carries a huge amount of personal data (i.e. data from the user, such as photographs, contacts, messages or even financial information), and/or confidential or reserved information from the professional life of the device owner (i.e. professional contacts, e-mails, documents, etc.). The access to all that information should be protected in a way that only the authorized person is able to access it. Therefore, authentication mechanisms should be used. A third-party may observe PIN code or gestural pattern entry, as mobile devices are frequently used in public places. The use of tokens have not been so widely implemented in mobile devices, as interfacing with the token will be accompanied by a set of usability constraints, due to the need of a connection slot for such token (i.e. a smartcard reader connected by OTG or Bluetooth). In addition, such token might be lost, stolen, or even copied.

Biometrics can be used to ease such a process, as long as the device is equipped with a biometric capture device (i.e. sensor). The user's biometric reference is also a piece of personal data that has to be protected from a non-authorized access. The direct access to the biometric reference may facilitate an attacker to impersonate the user of the mobile device, either in such a device, or in any other authentication process that may use that same biometric characteristic.

The reading or copying of credentials should be denied. Also, there should not be any possibility of overriding the authentication process. It is then when the traditional vulnerabilities of IT solutions are shown. As most of mobile devices are general purpose platforms, with the possibility of downloading any third-party application, it is feasible to get Trojan horses that may implement man-in-the-middle attacks, to manipulate data or the authentication process.

In addition, analogously to the case of copying of the user's PIN code or gestural pattern, biometrics may be "copied" and re-used by an attacker. Biometric data, in most cases, is publicly available (e.g. latent fingerprints, face photographs, iris photograph at a distance, etc.). Therefore, an attacker could obtain the raw information from the user and create artificial samples from it, trying to gain access to the system. This is usually known as presentation attack, or spoofing, requesting the need to include presentation attack detection mechanisms during the biometric acquisition process. More information on presentation attack detection may be found in ISO/IEC 30107.[7] The target of those mechanisms is to detect, and therefore deny, the presentation of samples that may be subject to be considered as artificial. In mobile devices, biometrics are only intended as being an authentication mechanism, not identification. Therefore, attacks such as obscuration (i.e. avoiding being identified) are out of the scope.

Although achieving 100% data protection is practically impossible, many things should be implemented to improve the level of privacy achieved in current devices.

The first question is whether the best authentication method is being used at the appropriate time for the application. It is not the same to authenticate yourself for unlocking the device, than to perform a bank transfer. Also it all depends on what information is stored in the device or not, so that being able to unlock the device may mean a much bigger threat than a non-authorized transfer.

Going into detail, it is important to highlight that biometrics may be used alongside a token-based approach to improve protection. All GSM mobile devices already include a smart card (i.e. the Subscriber Identity Module – SIM), that could be used for storing identity credentials and personal data. But it is also true that the SIM is dependent on the mobile operator, and also not thought to be extracted from the device, so that if the device is stolen, the token is also stolen.

A new viable possibility is the use of other kinds of external personal tokens, such as contactless smartcards, that could be able to connect with the mobile device using interfaces such as NFC (Near Field Communication) or BLE (Bluetooth Low Energy). In that case, the user can carry that token in his/her wallet, and the device being able to connect with it without the need of using additional peripherals. In that case, the smart card can be empowered with public key cryptography, so as to be able to perform not only Authentication, but also Digital Signature. In order to authenticate yourself to the token, PIN codes could be used, or even biometrics, whenever the token has on-card biometric comparison functionalities (see ISO/IEC 24787).

Independently of using or not external tokens, further actions should be considered as to provide a higher level of data protection. Going from the side of the user (the user's interface) till the operating system, several improvements are available. The first thing to consider is the way the device can be locked when not in use. Currently, strategies regarding PIN codes and, in particular, gesture patterns are widely used. Such unlocking mechanisms are subject to be copied by overlooking during the process of unlocking. Some of the users already are aware of this, but they do not consider it a security process, rather much more as a way to avoid undesired calls while carrying the device in a pocket or handbag. Most users prefer the gesture patterns due to the ease and speed of entering them, or common PIN codes such as 1212 (easy to type without even needing to look at the screen). These considerations give rise to the most important requirements that an unlocking procedure should comply to: friendly, easy to remember, easy to enter and fast. If any of those requirements are not fulfilled, then the probability of a user choosing an easier version or even overriding the whole process is very high. As the unlocking process of the device is the first step in the security of the data and processes hosted in the device, new solutions should be considered.

With the appearance of commercially available touch verification technology on smart devices, a new alternative was demonstrated. Placing the finger on the sensor is user friendly, easy to remember, easy to enter, and if the algorithm is fast enough, in less than a second for instance, the process can be very convenient for the user. The non-cooperative creation of a fake sample is difficult and slow, so this method of attack is considered unlikely for the unlocking process so the privacy level achieved is much higher.

Protection of any credentials stored should also be addressed. If third-party software is able to access the identity credentials, the user's privacy will be compromised. This protection can be achieved by the use of Secure Elements (SEs), such as smartcards or specific parts of the device microprocessor built for holding security information. SEs can be manufactured in a way that the security information will never be read, but only internally verified or processed (e.g. as with the PIN codes or private keys in a digital signature scheme). Such SEs could be internal or external, and could hold more or less data. What it is important is that the operating system of the device, can only access such SE under security conditions, and that the best practices in terms of security are followed during the operation of the mobile device. The incorporation of those SEs and the mentioned security rules is what is called a Trusted Execution Environment (TEE).

Regardless of the quality of the TEE on the mobile device, there are further risks to privacy and data security which occur if any biometric information is transmitted to a central server. In this case, it is essential to properly authenticate the central server and to encrypt any biometric data that is transmitted. It is also essential that the central server and the entities controlling it ensure that proper security protocols are in place. Historically, most data breaches have occurred once data for multiple

users has been accumulated in a central location. It is important for any application to therefore consider the additional risks when biometric data is transmitted to a central server rather than remaining on the mobile device.

There are several strategies for developing a TEE, but most of them conflict with usability and users' needs or preferences. The most radical strategy is to provide the mobile device with the only set of applications allowed, as they are already developed by the device manufacturer and, therefore, their best practices double checked. This strategy will, nowadays, not be accepted by users because of their willingness to install new applications that they consider of interest. The second strategy could be to force that all applications to be installed in the device should come from an authorized and verified source. This will make application developers follow a kind of certification scheme for their applications, which will, in many cases, impose the need to charge users for the use of them. This strategy presents the following secondary effects: a) the device manufacturer has to certify ALL applications developed, requiring an increasing amount of resources that may not be justified by the depth and complexity of many of those applications; b) some users may consider the ability to use non-certified applications more important than security. A user should be made aware of the losses in security and data protection that they will suffer: there is a need of education for the mobile device users.

There is a third alternative that divides the device into two independent environments: a) a secure environment with independent storage memory and certified applications, i.e. the TEE; b) a non-secure environment where the user may install all those applications that he/she may want, and which has no direct access to the data stored in the TEE. Simply by pressing a button, the change of environment is achieved, and each environment is identified by a different set of colours, so that it becomes easy for the user to operate the device achieving a reasonable level of data protection.

It may be an enhancement to protect the change of environment (in particular, activating the TEE), by a certain kind of authentication. But in such case, the same usability problems as described above may appear, so the use of a biometric characteristic for such task may be of benefit.

An alternative to the use of TEEs for securing biometric templates stored at mobile devices is the use protected templates.[7] [8] These schemes store biometric templates in a non-invertible form. They are usually divided between biometric cryptosystems and cancellable biometrics. Biometric cryptosystems provide mechanisms also to bind or release cryptographic keys. Desirable properties of these template protection schemes are renewability and revocability, besides the aforementioned non-invertibility. The use of these kinds of schemes is not specific to TEEs or SEs, thus, avoiding the adaptation of the biometric system to different environments, which can ease the integration of the biometric system. More detailed information may be found in ISO/IEC/TR 24714-1.

Last, but not least, if data protection is going to be guaranteed by the use of biometrics, presentation attack detection should be addressed. In this case, it is necessary to perform a vulnerability analysis and to assess the attack potential for each identified vulnerability.

To detect presentation attacks, either additional sensors should be integrated in the device, or the biometric acquisition should be carried out in a continuous way, as to detect both, human perturbations in the samples that are not present in artificial samples, and sample perturbations created by the presence of artificial layers over the real biometric characteristics of the attacker.

Privacy and personal data protection issues with the use of biometric and other supporting data need to be addressed. More detailed information may be found in ISO/IEC/TR 24714-1 and ISO/IEC 30107.

5.2.3 Biometric sample capture

The acquisition of biometric data, i.e. the integration of the biometric capture device in the mobile device is a challenge which depends on the biometric modality. The use of touch screens allows an immediate integration of modalities such as handwritten signature, touching patterns or keystroke dynamics. Also, the use of the attached camera in most mobile devices, allows the costless integration of face recognition or peg-free hand geometry recognition. Other sensors that are commonly integrated in current mobile devices are accelerometers and gyroscopes. With such sensors, gait[10] or signature on the air[11] can be implemented. And obviously, the use of the device microphone can be used for speaker recognition.

The size of the screen, as well as the place where the user has to sign, may imply that the user touches the screen with the wrist when signing, which may impact the information captured, or even can stop it. The illumination conditions at the time of acquiring a face photograph (e.g. strong back light) may create invalid face image samples. Also, the lack of an image stabilizer may also lead to get blurred samples, impacting seriously the performance. In the case of gait, the location of the mobile devices is one of the parameters that affect greatly the information captured, while the way the smartphone is grabbed, implies changes in the gesture information of the signature on the air. Therefore, further work is needed in this area.

There are other biometric modalities with no generic sensor embedded in the device. Some modalities, such as fingerprint or iris, have attracted the interest of the device manufacturers, which are integrating some biometric capture devices. In some of the cases, these capture devices can only be used by native applications, and therefore useless for third party applications.

As for vascular, some laptops and tablets equipped with a built-in vascular sensor already exist as commercial products. Other modalities are in the research and prototype phase, or need external capture devices connected either through OTG (On-The-Go – the USB connector of a smartphone), or Bluetooth.

5.2.4 Sample authentication process

Many things have already been said in this Technical Report about the requirements to acquire biometric data. In summary, the developer should provide the means to authenticate the user that suits his/her needs minimizing the demand for interaction, and the fastest and most reliable operation. The use of external biometric capture devices should be discouraged, but if this is not possible, at least a wireless interface should be used. In this case, cyphering of the exchanged information is a major requirement, as to avoid man-in-the-middle attacks.

It is important to analyse the operational conditions as to adjust the requirements for the biometric capture device. Parameters such as temperature, humidity, lighting conditions (including the effect of direct sun light), vibrations (e.g. while walking, being on a train, etc.), or noise should be deeply studied.

In addition, the authentication process, and in particular its complexity, should be designed in accordance to the application needs. It may be of interest that each of those needs require a different kind of authentication, being even recommendable to require more interaction when something sensible is trying to be accessed. Therefore, a possible strategy may be that one of a user-friendly biometrics for unlocking the device, then a wireless token-based authentication for accessing bank details, and an on-card biometric comparison scheme for allowing and signing money transfers.

Of much more importance is to develop solutions using a user-centric design. All authentication processes should pursue the target of being easy to use, easy to interact, easy to remember, and fast in its execution. Obviously, some security needs may affect the level that target could be achieved, so the designer should be able to balance security with usability. Also, an important consideration is the variability of users involved in the process, which also includes dependent people or people with different kinds and levels of disability. Applications, and in particular, the authentication process, should be designed in a way that its user interface can be adapted to the needs of the user (e.g. visual and auditory feedback, different fonts and sizes, different contrast, etc.). Recommendations such as the ones in ISO/IEC/TR 29194 should be followed. In cases of disabilities, the use of external devices for approaching the recognition to those users with lack of mobility or inability to hear or see, may be a recommended solution.[12]

Finally, to improve usability, it is recommended that a common interface is used for all applications. The authentication usability would be improved if it is directly provided by the operating system. This will not only help in securing the process, but also in creating a common way of interaction between the user and all the applications, which will ease the process, and as well will create a trust link during the authentication.

5.2.5 Usability

5.2.5.1 General

There is a range of unique attributes in mobile computing that provide a user experience somewhat different to that of desktop computing that developers should consider.

An initial distinction to draw between mobile and desktop usability relates to the wide variety of mobile devices. If we consider a mobile device is one that does not require a user to be in a specific location, this introduces a broad spectrum of devices, which may include laptops, tablets, phones and wearables. Each of these devices of itself has different modes of use, however this Technical Report will limit itself to the generic attributes that apply to tablets, phones and wearables.

5.2.5.2 Ambient conditions

Mobile applications are used in a variety of conditions that are generally not controllable. The effect of these conditions on the use of the device should be considered. For instance, speech capture will be affected by extraneous noise (e.g. wind, third party speech, background sounds) while visual capture will be effected by light, reflections, people and items in the background and movement.

5.2.5.3 Reduced screen space

The reduced display size of mobile devices requires developers to focus on identifying the core visual cue required at a particular point in time and to reduce all extraneous visual information. Reducing the level of visual information on screen requires that the developer has a solid understanding of the application's workflow and what information a user should be presented with at any one point during the application's workflow.

5.2.5.4 Limited input options

Due to the small form factor, a mobile device will by necessity reduce its range of input options to take greatest advantage of its limited overall size. This has led to various strategies when addressing input requirements, where it is now common for tablet and phone type devices to present a textual input mechanism as part of the screen. While this strategy reduces the need for additional keyboard type devices, it does impact on the limited screen real-estate offered by these devices. An understanding of the application's workflow is necessary to ensure the presentation of an on-screen keyboard does not negatively impact on the visual feedback presented to the user.

Other input options, such as a microphone, camera, accelerometer and fingerprint sensor are present in various devices and while these are typically useful for a number of applications, for situations that require high fidelity capture (such as biometric capture, be that speech, face or finger) consideration should be given to several aspects:

a) whether the input device is technically capable of capturing the information at a sufficient level of fidelity and at what distance;

b) whether sufficient instructive information can be provided to the user to ensure they capture the sample at a sufficient quality;

c) whether the user has the inclination or ability to capture the sample to the desired quality.

5.2.5.5 Limited processing capacity

While mobile devices are undoubtedly high powered pieces of equipment when considering only their raw specifications, that power is quickly diminished through the introduction of operating systems presenting highly interactive user interfaces. When compared to a desktop application, the mobile application will have significantly less resources and speed of operation with which to work.

Mobile applications, particularly those that are 'ports' from a desktop version, need to pay attention to operating with limited processing power and memory. An application that results in a user waiting for processing to take place, and appears unresponsive to a user, will naturally be considered by the user to be broken or faulty. Measures should be introduced in the first instance to make the application more responsive through using less resources. Alternatively cues could be introduced to the user interface to indicate that the application is actively processing, giving an indication the application is doing 'something'.

5.2.5.6 Connectivity

Connectivity (to external resources) should be seen as a potential issue for use of a mobile application. Applications reliant on external systems to perform processing should have some method of running in an 'offline' mode or clearly indicate to a user that an external resource is not available. If the application is completely dependent on an external resource, it must present clear and unambiguous methods to indicate whether a connection is present and to test the connection to verify the connection's integrity. The application must also incorporate robust error handling for loss of a connection mid-transaction, where neither the transaction nor application itself should be seen to fail. Users will perceive applications that fail due to connection issues or lose of data, to be faulty and hence not suitable for use.

5.2.5.7 Cognitive load

An interesting new dimension that mobile devices bring to the discussion of usability, which deviates from traditional desktop computing, is that of cognitive load.

Whereas a user will engage with a desktop computer as a sole task, it is not unusual for mobile devices to be used while users are performing some other actions (e.g. driving a car and using a navigation app on a mobile phone, walking while texting). The introduction of users performing parallel actions whilst computing should be considered during an application's design. As additional simultaneous tasks are introduced a user's total cognitive ability will be split between those tasks. This requires applications present the most applicable interface at any point during an application's workflow to ensure extraneous actions (such as button clicks, screen changes and other visual noise) are reduced to a minimum to so the application provides the richest set of information while minimizing unwanted distraction.

5.2.5.8 Consumable context

The way users think about mobile applications, and their attention span when trying out new 'apps', brings another new aspect to the usability of mobile applications.

All major mobile OS platforms have introduced the concept of "app stores" which present a wide variety of applications to address a range of computing needs. Given the volume of applications available in these stores it is not unexpected that mobile users treat mobile apps as a more disposable product, than say a desktop application. After all, if one app fails to meet expectations, there will undoubtedly be many more to trial. The paradox is that, as many of the apps are free, they are typically of low quality. This immediately trains users into thinking mobile apps are disposable, low quality products that should be quickly churned through to find a solution that works. Through this commoditisation of 'apps' and the huge choice of applications, users of mobile applications can typically be expected to have a low threshold for tolerating poor design, or even a design that doesn't immediately capture their attention. If one app does not work a typical reaction would be to delete it and install a substitute.

To assist in making the app 'sticky' (i.e. making the app exhibit a greater number of desirable than undesirable traits), developers need to address the unique properties of mobile computing usability.

More information on user interaction with mobile biometrics can be found in References [13] and [14]. There is also a standard for assessing accessibility in ICT products (EN 301 549), including mobile biometrics[15] and NIST has published usability in biometrics guidelines.[16]

5.2.6 Solution testing

It is also important to determine the level of accuracy of the integration of biometrics. This should be done not only by evaluating the algorithm with a set of samples from a database, but also including the biometric capture device and analysing the interaction of real users with the mobile. It should be mandatory to carry on not only a technological evaluation, but also a scenario evaluation (using ISO/IEC 19795).

The technological evaluation should also include the evaluation of the security achieved by the solution, searching for vulnerabilities not only at sensor level, but also at the operating system level.

The first main challenge comes from the need of executing the algorithm in the mobile device, which will consume a lot of time when major databases are used. The second main challenge comes from the need of evaluating the security of the whole operating system, with a major focus on the storage of information, the access to that information, and the exchange of information with the outside world.

During the scenario evaluation, it is of much importance to analyse the usability of the solution, which means using real subjects in multiple sessions and multiple scenarios and positions. This means long lasting and expensive evaluations. But it also drives other challenges. One of the important facts in the evaluation of the usability of a system is to analyse its level of usability for technology newcomers, i.e. citizens that have not been previously involved with this kind of devices and with biometric authentication. As technology expands its deployment, this will become less and less possible, as most of the users will have had access to the technology.

Last, but not least, devices change very fast as models evolve due to marketing reasons. The new models imply changes in size, in peripherals, computational power, user interface and operating system. These changes may impact the performance of the system under operational conditions. Obviously, it would never be possible to test the system in all possible devices, so an evaluation strategy to minimize the effort maximizing the conclusions extracted should be defined.

5.2.7 Challenges common to other scenarios and platforms

In addition to all the previous challenges, the typical ones from any other IT application applies. In particular, it is of much importance how the integration of the biometric authentication should be done in each of the applications. The target is to maximize the return on investment (ROI) so that such ROI increases the benefits and reduces the time in obtaining those benefits.

In order to reduce the implementation costs and, therefore, improve the ROI, a standardized API is needed. In biometrics, the only standardized API for developing application is BioAPI, which was published in the standard ISO/IEC 19784. Unfortunately, this API was defined in ANSI C, without considering object oriented programming languages, and no free reference implementation is available. Fortunately, there are currently works in the development of an Object Oriented version of BioAPI, defined in UML, and also specified in Java and C#. These works are targeting the creation of the ISO/IEC 30106 family of standards.

There are currently beta versions of the reference implementation that have even created Object Oriented BioAPI applications under Android-based systems using ISO/IEC 30106-2, which is the Java specification. All information about these reference implementations can be found in Reference [17].

Another aspect in reducing the implementation cost is the evaluation of the solution. By using a common authentication process to all applications, the impact of this cost can be minimized. Also, the use of the new advances in the creation of a methodology for evaluating biometrics in mobile devices, in particular considering usability,[6] will help to reduce the evaluation costs improving, at the same time, the reliability on the results.

6 Biometrics services within the OS of the mobile device

This Clause describes several options of implementing biometric functionality within the operating system of the mobile device from an abstract point of view. This list is not exhaustive and other implementations may exist.

Considering a generic architecture of a generic operating system (OS) as shown in the Figure 1, this Clause relates to the case where the biometric interface (BI) is developed at the low-level libraries level, with direct access to the OS kernel and therefore a first level indirection to the hardware through the Hardware Abstraction Layer (HAL).

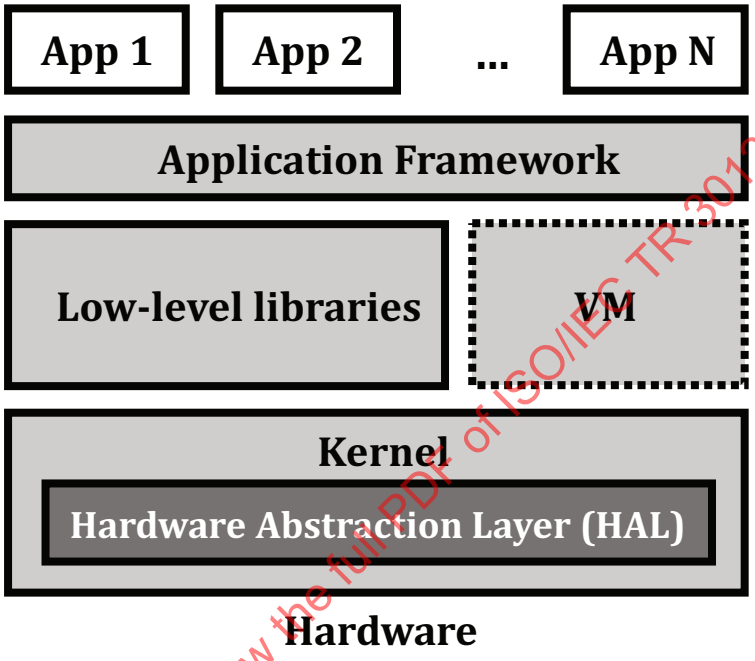

Figure 1 — Generic architecture of a mobile device OS

The OS manufacturer is able to provide the BI accessing all resources available in the hardware, and offering those biometric services at the Application Framework, so that applications could use those services by calling the relevant Application Programing Interface (API). This is represented in Figure 2.

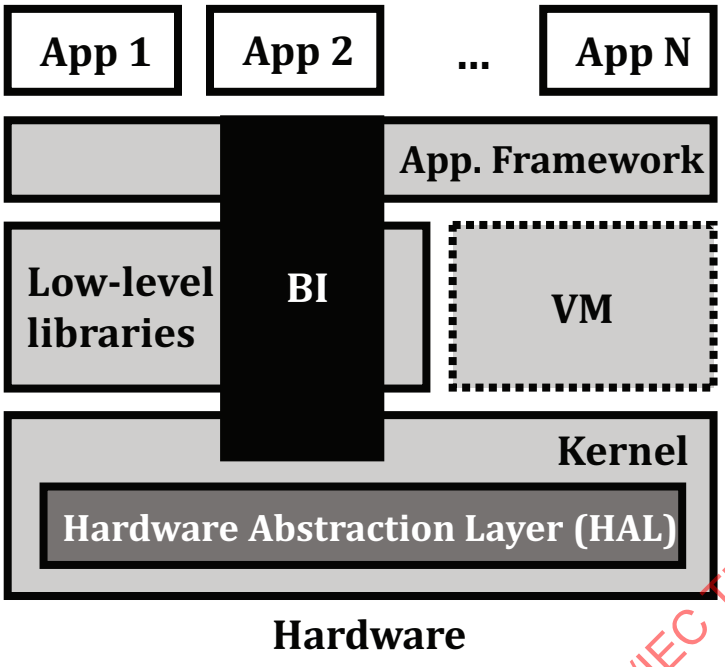

Figure 2 — Location of a BI when developed within the OS

In those OS where a Virtual Machine (VM) is available, and the OS manufacturer is willing to provide the BI services for applications being executed at the VM, a link between the VM and the BI may be established.

In order to be able to provide a certain level of assurance, the BI should be developed as in a sandbox, where no other service may tamper with the BI implementation. Also, access to the BI functionality should only be available through aggregated functionality methods, such as:

— Enrol a biometric reference (i.e. enrol a user);

— Verify an acquired sample with a previously stored biometric reference;

— Identify an acquired sample within the set of biometric references stored at the device;

— User interaction through callbacks (or similar mechanisms) that provide the Applications a Graphical User Interface (GUI);

— Exception handling for both system errors as well as user errors.

In the event that the OS can support remote biometric services, then the following should be considered.

— Provide a method to store a biometric reference provided by the remote server.

— Provide the atomic functionality to capture a biometric sample in the following ways:

  — either in a non-processed way or as a processed data record;

  — cyphered using a cryptographic protocol agreed between the device and the remote server.

— Incorporate, if possible, mechanisms to mutually authenticate the server and the device, in order to prove the validity and integrity of the biometric data exchanged.

The OS manufacturer may want to implement attack detection mechanisms and policies, so that the use of the biometric functionality may be inhibited (temporally or permanently) on detection of such attacks.

The OS manufacturer may provide a configuration functionality, by which different parameters are chosen for the use of the BI for certain applications and/or scenarios. For example, it may provide a discrete number of assurance levels, for which different decision thresholds (i.e. quality, comparison, presentation attack detection, etc.) are selected.

Internally, the OS manufacturer, in order to implement the BI, may create some of the following functionality:

— capturing one or more biometric sample(s) from a sequence of samples (i.e. a facial image from a live view of a face);

— establishing the best sample(s) based on some quality metric;

— providing a quality metric for sample capture;

— providing information on what sensors are available on device (e.g. camera, multi-touch screen, finger scanner, GPS, accelerometer etc.) together with any relevant technical details (e.g. touch screen resolution, number of multi-touches, camera resolution, etc.);

— providing information on what biometric modalities have been captured as references;

— comparison algorithms for each modality 1:1 and/or 1:few.

Consideration needs to be given to what elements may be resident on the device and what passes through to the web service. Different approaches may be taken in different circumstances, even for the same application. The device may be connected or not connected, although in this kind of approach, usually the BI is implemented using capture devices already available in the mobile device. At the platform level the user should see consistency in their interface.

There are many benefits of this approach, the two major ones being: a) the use of native code and the lack of intermediate layers that may induct a loss on performance; b) the direct access to all available secure elements in the device. This second benefit is extremely important, as the creation of a TEE by the OS, can make a bidirectional benefit between the TEE and the biometric services. The BI can benefit from being executed in the TEE, and therefore avoiding many of the potential attacks (in particular those based on man-in-the-middle approaches). In addition, the BI can benefit from being able to use the low-level Secure Elements that may store securely all biometric references. On the other hand, the TEE can benefit from the BI in having an additional user authentication mechanism, which relies more on who the user is, instead of on what the user knows or what the user possess.

7 Biometric services at the application level in a mobile device

In those cases where the BI is not included in the OS, or there is an interest of using a different BI than the one provided by the OS (e.g. because of using another modality, or due to trusting more the solution coming from a third-party), the BI should be developed at the application level, as shown in Figure 3. In Figure 3, it can be seen that the BI is located at the same level of the rest of applications, but providing shared services that can be used by other applications (i.e. App H till App K). Other applications on the device can co-exist, not using the BI, such as the ones named in the figure as App 1 and App N.

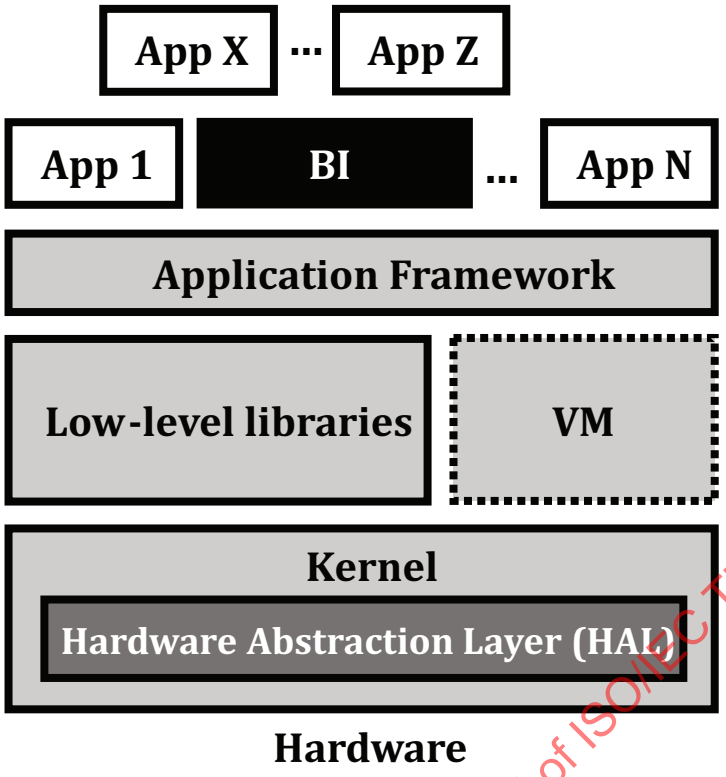

Figure 3 — Location of a BI when developed at the Application Layer

In this case, all recommendations given in Clause 6 are applicable to here, referring to the BI manufacturer in those places where the OS manufacturer is named. But in addition to all those recommendations, some others apply in this case:

a) The OS should allow that the Application Framework to create the BI in a sandbox that denies access from other applications to its functionality outside of the shared interface provided.

b) The OS should allow that the biometric capture device, which belong to the Hardware layer, is accessed temporally in an exclusive way, so that while the acquisition process is running, no other application or service can access such hardware, neither the memory reserved for such process.

   The biometric capture device can be internal or intrinsic to the device (e.g. a touchscreen, a microphone, etc.) or even external through a communication interface (e.g. OTG, Bluetooth, etc.)

c) As with the biometric capture device, the module used for storing the information should also be accessed temporally with exclusivity when storing or reading the biometric reference. It is recommended that the module used for storage allows storing the information in a cyphered way and through internal authentication mechanisms (such as those included in many smartcards).

In this kind of approach it may be more difficult to build a TEE using the BI, but if the OS provides such TEE, it is recommended that the BI is installed inside such TEE.

Also, when developing the BI, and in particular for implementing the biometric algorithms, it is recommended to use native code (whenever possible) as to reduce as much as possible the execution time latency when performing biometric operations.

8 Biometric application development [using the biometric engine(s) provided]

Although proprietary APIs may be offered by either the mobile device manufacturer or the operating system provider, the use of standardized APIs is recommended to allow interoperability among developers and remove the need to adapt the biometric solution to different devices and applications.

ISO/IEC 19784-1, most commonly known as BioAPI 2.0, comes from the input of the BioAPI Consortium, which previously developed the high-level biometric API that was called BioAPI 1.1.

Where in Clauses 6 and 7 was described the definition of a BI, such BI should be connected to a Framework, which may be developed by, either the OS itself, or a third-party application. In the case of the ISO/IEC 30106 Framework being implemented by the OS, such Framework should allow that the BIs are developed not only inside the OS, but also as an application-level service provided by a third-party, which shares the interface only with the Framework, not allowing its access by other applications. Then the applications willing to use BIs should request that by calling the Framework API defined in ISO/IEC 30106. This is represented in the following Figure 4.

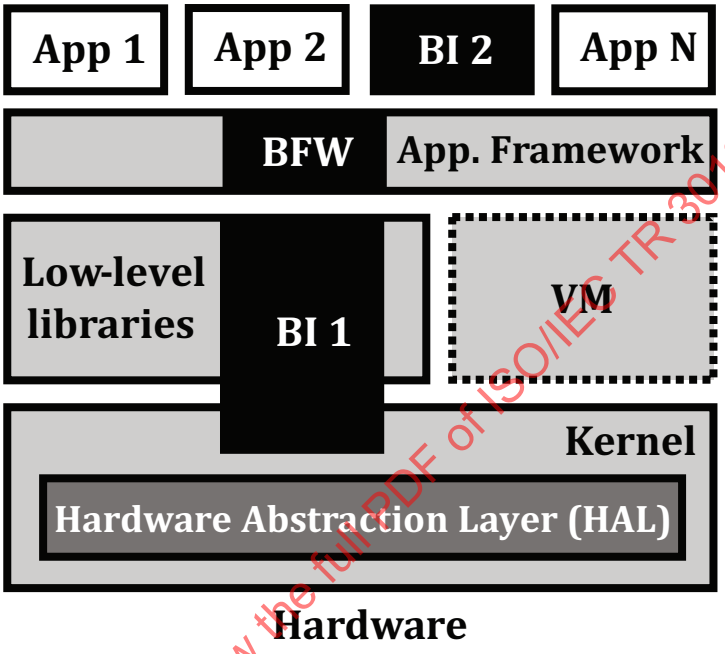

Figure 4 — Illustration of a way to include the ISO/IEC 30106 Framework (BFW) within the OS

In case the Biometric Framework is not included in the OS, then a hierarchical illustration of one way to implement this solution is shown in Figure 5:

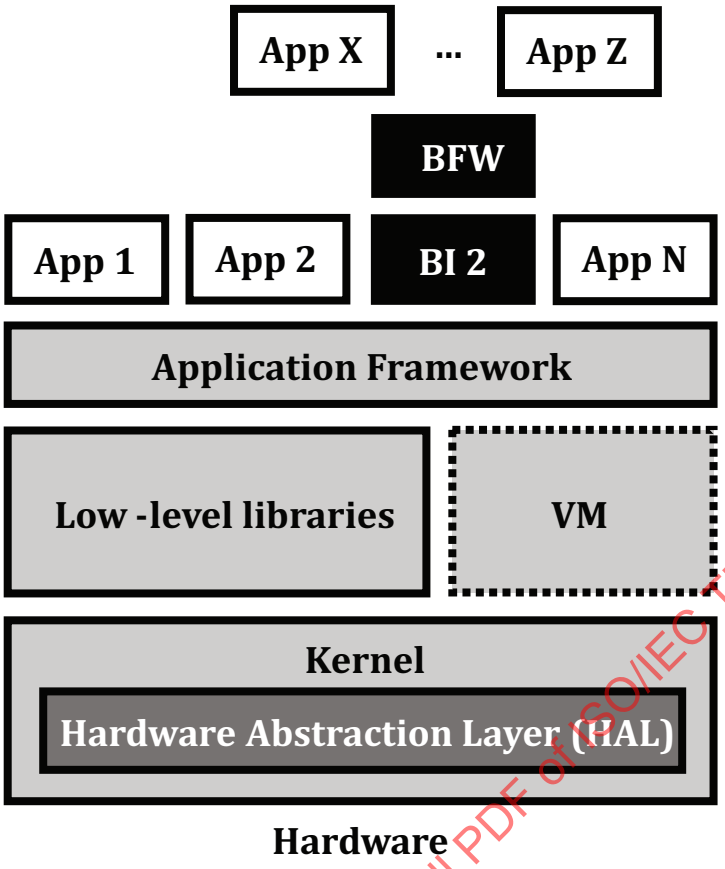

Figure 5 — Illustration on how the ISO/IEC 30106 Framework (BFW) may be implemented at application level

An important topic to address is the interaction between the BI and the application, in particular when dealing with the user interaction. Although not recommended, a BI may handle by itself the interaction between the user and the system. For example, a BI with a biometric capture device may address all the interaction by the displaying messages, illuminating LEDs and/or activating sounds at the sensor itself. Such kind of interaction may include providing feedback to the user on

— the finger to be placed at the sensor,

— how to improve the location of the sample in the sensor (e.g. alignment of the biometric characteristic in relation to the sensor active area),

— whether the acquisition has been done in a correct way, or

— whether the biometric comparison has led to a positive or negative decision.

But in most cases, it may be requested that such interaction is handled by the application using such BI, showing all messages and illustrations in the device screen, in order to avoid being handled by the BI itself and leading to certain kinds of inconveniences such as

— the BI graphical user interface may not be adaptable to the different sizes and resolutions that the application screen is using,

— the feedback provided has to follow the same look & feel as the main application, including the use of service provider logos,

— the feedback has to be adaptable to the language of the user being identified, or where the system is deployed.

In those cases, the way to solve this is by using callback functions. Callback functions should be designed for each step where the BI requires to interact with the user, and for each of the processes to be called, the application provides the BI with the selected functions, so that the BI can call them within the execution of the process. Therefore, if the BI allows the use of callback functions for handling the GUI, the following development actions should be taken, for each of the processes requiring such interaction (e.g. capture):

The application should implement all GUI related functions for such process. These functions are of the following kinds.

— Select Function: to show the interaction with the user at the beginning or the end of the whole process. For example, at the beginning the process, the following message may be provided: "Capture process for the index finger of the right hand". And at the end of the process the message to be given could be: "Acquisition finished. Thank you!". Therefore, the callback function should know if it is being called at the beginning of the process, or at the end. Also the callback function can also provide the BI with information about a user action, such as cancelling the capture process. All this information flow is provided in parameters of the callback function.

— State Function: Sometimes the BI process may take several internal steps, which can be designed as different states. Therefore, the state function will provide feedback depending on whether a certain internal step is to be started or finished. This leads to the need for the State Function to know which internal step is being processed, and that information will be provided as parameters to the callback function. Also feedback provided by the user will be passed to the BI by the parameters involved, such as cancelling the whole process.

— Progress Function: In some other cases, it may be necessary to provide the user with real time feedback on the progression of the process. For example, a system may be showing in the screen the live image of the fingerprint or face within the acquisition process. In such case, a Progress callback function may be implemented to show the data stream.

Once the callback functions have been implemented for the process, the application should report the BI about the callback functions to be used, before calling the process. This will be done by subscribing the BI to those selected GUI events, and the relevant callback functions. Once subscribed, the application can call the process (e.g. Capture). Finally, when the process has been completed, the application can unsubscribe the BI from the previously subscribed events.

An application developer should be aware of the operations and options that the BIs included in the application offer, in order to know which of the methods should be called. The application developer should also check the exceptions occurred with any call to any method, and check whether the called functionality is available in that BI, or any other kind of error has occurred. It is recommendable, for simplicity of the application code, that the application developer uses the highest level methods available, e.g. those in which all the biometric data is handled within the BI and not circulated through the application.

In addition, it may be beneficial to use web services at a variety of system component interfaces. This would not only improve interoperability but allow biometric capabilities into systems that might not otherwise have them available. For example, an acquisition service such as WS-Biometric Devices would allow a mobile device without a built-in fingerprint scanner to acquire fingerprints from such an enabled scanner. A standard web service such as BIAS (ISO/IEC 30108-1) may do the same for enrolment or recognition; for example, in cases where the data or comparison capabilities are not available locally. (Further information may be found in NIST/SP 500-288 v1.)

9 Functional and operational guidance

9.1 General guidance

9.1.1 Guidance on functional architecture

Although there could be many functional architectures envisaged this Technical Report will be limited to the following key aspects.

a) A data subject will register only once with an application for each device (e.g. laptop, tablet, and smart phone).

b) A reference can be stored locally on the device or on central servers (in the cloud).

c) Authentication can take place locally on the device or on central servers (in the cloud). (The authentication context is provided in ISO/IEC 24761.)

d) If the application requires authentication to be performed even if the device is off-line (i.e. no connectivity), then registration details, including biometric reference data, will be distributed to all instances of the application on the data subject's devices, via a Cloud Data Management Interface.

e) When the near field communications are used to initiate an authentication process then the transaction will exchange sufficient data to enable the establishment of a secure communications channel (e.g. Wi-Fi, GPS) for sufficient 'challenge response' communications to take place.

f) This Technical Report is limited to architectures supporting 1:1 authentication and 1:few recognition.

g) Capture may occur on device or from a physically or logically tethered sensor.

In the Internet environment, the result Success/Failure from the client may not be trusted by the verifier without certain conditions because the execution environments depend heavily on users which may include attackers. Therefore, evidence of an authentication result is necessary for the verifier to trust it.

9.1.2 Guidance on environmental conditions and constraints

In the vast majority of 'fixed' biometric applications, enrolment and verification of the subject takes place in a controlled environment where lighting, temperature, humidity, background noise etc. can be optimized to increase the likelihood of obtaining a high quality biometric sample.

By their very nature, biometrically equipped mobile devices will be used in a wide range of environments; indoors and outdoors, during the day and at night, in bright sunshine, overcast, in the rain, snow etc., and the user (having paid for such a device and enrolled their biometric data) will in all cases still expect this aspect of the device to operate correctly.

The impact of environmental factors will vary with modality; bright sunlight may adversely affect face, iris and even fingerprint based systems, while high levels of background noise will inevitably have an impact on devices employing voice recognition.

See Clause 11 for details.

9.2 Guidance for enrolment

9.2.1 General guidance for enrolment

Existing 'best practice' guidance (ISO/IEC/TR 29196) has been designed to support interoperability and biometric searching across different applications and systems, and corresponding biometric sample quality metrics have been developed to help ensure conformance.

9.2.2 Supervised enrolment

In certain scenarios it may be desirable to enrol the user in a platform external to the mobile device and under supervision. One example of this kind of situation may be a banking application where the requirement is to enrol at a bank branch and then download the biometric information into the device of the user. This kind of scenario may help the client in changing the mobile device without having to repeat the enrolment process in cases when the downloaded biometric template has interoperability between the previous one and the new one.

Potential advantages of this approach may be:

— Avoiding the repetition of the enrolment process;

— In a supervised enrolment, the operator has the opportunity to provide the client all the relevant information and training;

  — Addressing any doubts and questions that the client may have;

  — Showing the client how to interact with the sensor and the application;

— The operator can apply available mechanisms to check the identity of the client, mitigating identity theft;

— Assisting the user to enrol to best effect, considering the different situations that the user will have to face for a later recognition.

The following should be considered.

— The communication and installation of biometric data into the device of the user should be done in a protected way. If that installation is to be done remotely the information should be cyphered and mutual authentication of both the server and the device should be carried out.

— From the pure biometric perspective, if the enrolment is done in a platform different from the one of the recognition, the processing and/or comparison algorithms will have to handle any differences in the sample acquired. Different sensor characteristics may impact the sample acquired and therefore the performance of the biometric recognition.

Differences in external ambient conditions between enrolment and the use of a mobile device for a recognition attempt may seriously impact performance. This should be taken into account when designing the system.

9.2.3 Unsupervised enrolment

While mobile devices may increasingly include biometric capabilities such as a fingerprint sensor, camera for face or iris recognition there is no guarantee that individuals will follow the manufacturer's instructions on how these should be used.

Existing 'best practice' guidance (ISO/IEC/TR 29196) has been designed to support interoperability and biometric searching across different applications and systems, and corresponding biometric sample quality metrics have been developed to help ensure conformance. However, in the case of biometrics on consumer devices users will inevitably experiment to see what will be accepted. For example they may try various facial expressions, pointing the camera at their ear or other parts of their body, using the side or tip of a finger rather than the flat part and so on. It is also possible that they may not even use a biometric (in the accepted sense of the word) at all, perhaps attempting to place an inanimate object on the fingerprint sensor, or point the camera at a picture of a face rather than at themselves. Such attempts may or may not be successful depending on how the sensor has been implemented and what quality thresholds have been set.

For low security applications, like device unlocking, interoperability will not be the main issue; rather it will be reproducibility that will be the key. Whether or not a user follows the manufacturer's guidance on how to enrol their chosen biometric(s) will be less important than whether they can reliably repeat

the process for subsequent verification/authentication (possibly on multiple devices and in multiple environments).

Signature recognition is a good example to consider. There is no requirement for an individual to use their normal signature in a biometric application; all that really matters is that what they provide when first enrolling contains sufficient detail to individualise them, and that they can reliably reproduce it for subsequent verification.

However, this need to be able to accurately reproduce (for example) a particular gesture or facial expression if the system is to be able to recognize them on subsequent occasions may not be readily apparent to users who are unfamiliar with biometric technologies.

The use of unsupervised biometric enrolment on mobile devices also has implications for existing biometric quality metrics and it is possible that new quality algorithms would be required. For example these may need to be weighted more towards the complexity (and thus uniqueness) of the sample provided as well as the degree to which the user can reproduce it in a range of environments and across different devices, rather than whether it conforms to more conventional concepts of biometric quality that have been developed to support interoperability.

9.3 Guidance for authentication

9.3.1 Remote unsupervised authentication

Further guidance is provided in ISO/IEC 24761.

After enrolment, biometrics can provide greater assurance in unsupervised authentication of the enrolled individual's identity than other types of credential, because (as mentioned in the introduction of this Technical Report) they are linked or bound more closely to the person than are credentials such as passwords or tokens, which can be more easily stolen or lost.

To deliver this greater assurance effectively in a mobile environment, it is, however, necessary to implement robust technical security procedures in the design of all applications and transactions which use them, to ensure:

a) that the individual's relevant biometric characteristics (e.g. fingerprints or iris) are actually being captured "live" from the individual at the time when authentication is requested; this is to counter "spoofing", the fraudulent submission by someone else of stolen images or other representations of the enrolled individual's biometrics;

b) that digital data produced by the mobile application from biometric data captured in this process are certified as reliably linked to the timed process of capture from which the data are derived - this is to prevent another possible method of fraud, using data intercepted and recorded from previous transactions by the enrolled individual;

c) that the digital representation of the captured biometrics is produced in a one-way process, which does not permit data so derived to be used to create a synthetic image which could be used for other fraudulent authentication attempts;

d) where possible and appropriate, that the capture and processing of the enrolled individual's biometric data is being done on a mobile device which the individual is authorized and registered to use.

The security procedures summarized above for the capture and processing of biometrics on mobile devices for remote and unsupervised authentication must also be combined with appropriate follow-on procedures, to ensure:

a) that subsequent transactions in the identity authentication process preserve the integrity of the certified biometric data and any other submitted credentials;